REMARKS

Claims 1-9 and 13-20 are pending. Claims 1, 5-7, 9, 13, 16-17 and 20 have been amended. No new matter has been added.

I. Claims 1-9 and 13-20 are Allowable

The Office has rejected claims 1-9 and 13-20, at paragraph 2 of the Office Action, under 35 U.S.C. §103(a), as unpatentable over U.S. Patent Application Pub. No. 2002/0176579 ("Deshpande") in view of U.S. Patent Application Pub. No. 2003/0163733 ("Barriga"). Applicants respectfully traverse the rejections.

A. Claims 1-6

The cited portions of Deshpande and Barrigo, separately or in combination, fail to disclose or suggest the specific combination of claim 1. For example, the cited portions of Deshpande and Barriga do not disclose or suggest an authentication engine coupled to a network access hub via a global communications network, as in claim 1. The Office asserts that paragraph [0025] of Deshpande discloses this feature. *See* Office Action, page 3. Instead, Deshpande discloses that an authentication server 50 is connected to a hotspot service provider network or corporate intranet. *See* Deshpande, paragraph [0019]. The hotspot is a location where a wireless access point (e.g., a radio unit that connects devices wirelessly to a hotspot service provider's network such as Intel Corporation's PRO/Wireless 2011 LAN Access Point device) is strategically located for providing wireless devices and users of such devices, access to the hotspot service provider's network. *See* Deshpande, paragraph [0019]. Accordingly, the hotspot service provider network or corporate intranet is not a global communications network, as in claim 1. Thus, the cited portions of Deshpande do not disclose or suggest an authentication engine coupled to a network access hub via a global communications network, as in claim 1. In addition, the cited portions of Barriga do not disclose this feature. Instead, the cited portions of Barriga disclose artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066].

Further, the cited portions of Deshpande and Barriga do not disclose or suggest that the authentication engine is operable to issue a computing device a token indicating a grant of access rights to both transport services and federated data services of third party federated data service providers via the global communications network and the network access hub in response to authentication of an initial set of credentials without the user having to provide the initial set of credentials to re-authenticate with the third party federated service providers, as in claim 1. The Office asserts that paragraphs [0020]-[0022], [0025] and [0034] of Deshpande disclose this feature. *See* Office Action, pages 3-4. In contrast to claim 1, Deshpande discloses that a user registers a device with the intranet via the access point and access privileges are confirmed with one or more authentication servers on the intranet. *See* Deshpande, paragraph [0022]. The device can then request or accept email using one or more servers supplied through the access point and the intranet. *See* Deshpande, paragraph [0022]. With Deshpande, information (e.g., email, calendars, task lists, etc.) is not requested or accepted from a third party service provider, but is stored locally using a server on the intranet. *See* Deshpande, Figs. 1-4. The user will not be required to provide authentication information when physically moving into range from a first wireless hotspot to a second wireless hotspot to access the intranet if there is a current connection to the intranet. *See* Deshpande, paragraph [0025]. However, the cited portions of Deshpande do not disclose or suggest that re-authentication is not required to access a third party service provider that requires authentication, as in claim 1. *See* Deshpande, paragraph [0025]. Rather, Deshpande discloses accessing location based services (i.e., corporate intranet) using wireless hotspot technology and teaches away from authentication to access third party service providers using the initial set of credentials provided to access the location based services. *See* Deshpande, Abstract. Thus, the cited portions of Deshpande do not disclose or suggest that the authentication engine is operable to issue a computing device a token indicating a grant of access rights to both transport services and federated data services of third party federated data service providers via the global communications network and the network access hub in response to authentication of an initial set of credentials without the user having to provide the initial set of credentials to re-authenticate with the third party federated service providers, as in claim 1.

The Office admits that Deshpande does not explicitly disclose a token operable to authorize access of the user to the third party federated data service providers without the user

having to provide the initial set of credentials to re-authenticate with the third party federated service providers, as in claim 1. *See* Office Action, page 4. The Office asserts Barriga discloses this feature. *See* Office Action, page 4. Instead, the cited portions of Barriga utilize artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066]. However, artifact authentication is different from token-based authorization. Barriga's artifact does not indicate access rights to transport services and federated data services of federated service providers. Instead, Barriga's artifact method refers to a user's authentication assertion addressed for a single service provider. Thus, the artifact method does not disclose or suggest issuing a token indicating access rights to services of third party federated data service providers via the global communications network without the user having to provide the initial set of credentials to re-authenticate with the third party federated service providers, as in claim 1. Therefore, the cited portions of Deshpande and Barriga, separately or in combination, do not disclose or suggest at least one element of claim 1. Hence, claim 1 is allowable.

Claims 2-6 depend from claim 1, which Applicants have shown to be allowable. Therefore, claims 2-6 are also allowable, at least by virtue of their dependence from allowable claim 1.

Further, the dependent claims include additional features that are not disclosed by the cited references. For example, the cited portions of Deshpande and Barriga do not disclose or suggest that the federated data services include a first federated data service provided by a first third party federated service provider and a second federated data service provided by a second third party federated service provider, as in claim 5. The Office asserts that paragraphs [0019], [0025] and [0034] of Deshpande disclose this feature. *See* Office Action, page 5. In contrast to claim 5, Deshpande discloses "handshaking" with different hotspots of an intranet of a system, rather than accessing a first or second third party service provider, as in claim 5. In addition, the cited portions of Barriga do not disclose this feature. Instead, the cited portions of Barriga disclose artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066]. For at least this additional reason, claim 5 is allowable.

B. Claims 7-9

The cited portions of Deshpande and Barrigo, separately or in combination, fail to disclose or suggest the specific combination of claim 7. For example, the cited portions of Deshpande and Barriga do not disclose or suggest receiving a first set of credentials at an authentication engine from an electronic device of a user via a network access hub and a global communications network, as in claim 7. The Office asserts that paragraph [0025] of Deshpande discloses this feature. *See* Office Action, page 3. As explained above, Deshpande discloses that an authentication server 50 is connected to a hotspot service provider network or corporate intranet. *See* Deshpande, paragraph [0019]. The hotspot is a location where a wireless access point (e.g., a radio unit that connects devices wirelessly to a hotspot service provider's network such as Intel Corporation's PRO/Wireless 2011 LAN Access Point device) is strategically located for providing wireless devices and users of such devices, access to the hotspot service provider's network. *See* Deshpande, paragraph [0019]. Accordingly, the hotspot service provider network or corporate intranet is not a global communications network, as in claim 7. Thus, the cited portions of Deshpande do not disclose or suggest receiving a first set of credentials at an authentication engine from an electronic device of a user via a network access hub and a global communications network, as in claim 7. In addition, the cited portions of Barriga do not disclose this feature. Instead, the cited portions of Barriga disclose artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066].

Further, the cited portions of Deshpande and Barriga do not disclose authorizing access via an authorization engine to a third party federated data service provider via the global communications network and the network access hub in response to authenticating the first set of credentials, as in claim 7. The Office asserts that paragraphs [0020]-[0022], [0025] and [0034] of Deshpande disclose this feature. *See* Office Action, pages 3-4. In contrast to claim 7, Deshpande discloses that a user registers a device with the intranet via the access point and access privileges are confirmed with one or more authentication servers on the intranet. *See* Deshpande, paragraph [0022]. The device can then request or accept email using one or more servers supplied through the access point and the intranet. *See* Deshpande, paragraph [0022]. With Deshpande, information (e.g., email, calendars, task lists, etc.) is not requested or accepted from a third party service provider, but is stored locally using a server on the intranet. *See*

Deshpande, Figs. 1-4. Deshpande discloses location based services (i.e., corporate intranet) using wireless hotspot technology. *See* Deshpande, Abstract. Thus, the cited portions of Deshpande do not disclose or suggest issuing a token indicating a grant of access rights to a network transport service and to federated network data services of third party federated data service providers via the global communications network and the network access hub, as in claim 7.

The Office admits that Deshpande does not explicitly disclose a token indicating a grant of access rights to a network transport service and to federated network data services of third party federated data service providers via the global communications network and the network access hub, as in claim 7. *See* Office Action, page 4. The Office asserts Barriga discloses this feature. *See* Office Action, page 4. Instead, the cited portions of Barriga utilize artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066]. However, artifact authentication is different from token-based authorization. Barriga's artifact does not indicate access rights to transport services and federated data services of federated service providers. Instead, Barriga's artifact method refers to a user's authentication assertion addressed for a single service provider. Thus, the artifact method does not disclose or suggest issuing a token indicating access rights to services of third party federated data service providers via the global communications network, as in claim 7. Therefore, the cited portions of Deshpande and Barriga, separately or in combination, do not disclose or suggest at least one element of claim 7. Hence, claim 7 is allowable.

Claims 8-9 depend from claim 7, which Applicants have shown to be allowable. Therefore, claims 8-9 are also allowable, at least by virtue of their dependence from allowable claim 7.

Further, the dependent claims include additional features that are not disclosed by the cited references. For example, the cited portions of Deshpande and Barriga do not disclose or suggest authorizing access to the second federated network data service of the second third party federated data service provider in response to the subsequent request without the user having to provide the initial set of credentials to re-authenticate with the second third party federated service provider, as in claim 9. The Office asserts that paragraphs [0019], [0025] and [0034] of

Deshpande disclose this feature. *See* Office Action, page 7. In contrast to claim 9, Deshpande discloses "handshaking" with different hotspots of an intranet of a system, rather than accessing a second third party federated data service provider, as in claim 9. In addition, the cited portions of Barriga do not disclose this feature. Instead, the cited portions of Barriga disclose artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066]. For at least this additional reason, claim 9 is allowable.

C. Claims 13-20

The cited portions of Deshpande and Barrigo, separately or in combination, fail to disclose or suggest the specific combination of claim 13. For example, the cited portions of Deshpande and Barriga do not disclose or suggest an authorization engine communicatively coupled to a broad communications network and operable to issue a token operable as a valid indicator of access rights to both transport services and federated data services of third party federated data service providers over the broad communications network and at least one of the plurality of hotspots, as in claim 13. The Office asserts that paragraph [0025] of Deshpande discloses this feature. *See* Office Action, page 3. As explained above, Deshpande discloses that an authentication server 50 is connected to a hotspot service provider network or corporate intranet. *See* Deshpande, paragraph [0019]. The hotspot is a location where a wireless access point (e.g., a radio unit that connects devices wirelessly to a hotspot service provider's network such as Intel Corporation's PRO/Wireless 2011 LAN Access Point device) is strategically located for providing wireless devices and users of such devices, access to the hotspot service provider's network. *See* Deshpande, paragraph [0019]. Accordingly, the hotspot service provider network or corporate intranet is not a broad communications network, as in claim 13. Thus, the cited portions of Deshpande do not disclose an authorization engine communicatively coupled to a broad communications network, as in claim 13. In addition, the cited portions of Barriga do not disclose or suggest this feature. Instead, the cited portions of Barriga disclose artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066].

Further, the cited portions of Deshpande and Barriga do not disclose to issue a token operable as a valid indicator of access rights to third party federated data service providers and at

least one of the plurality of hotspots, as in claim 13. The Office asserts that paragraphs [0020]-[0022], [0025] and [0034] of Deshpande disclose this feature. *See* Office Action, pages 3-4. In contrast to claim 13, Deshpande discloses that a user registers a device with the intranet via the access point and access privileges are confirmed with one or more authentication servers on the intranet. *See* Deshpande, paragraph [0022]. The device can then request or accept email using one or more servers supplied through the access point and the intranet. *See* Deshpande, paragraph [0022]. With Deshpande, information (e.g., email, calendars, task lists, etc.) is not requested or accepted from a third party service provider, but is stored locally using a server on the intranet. *See* Deshpande, Figs. 1-4. The user will not be required to provide authentication information when physically moving into range from a first wireless hotspot to a second wireless hotspot to access the intranet if there is a current connection to the intranet. *See* Deshpande, paragraph [0025]. Thus, the cited portions of Deshpande do not disclose or suggest to issue a token operable as a valid indicator of access rights to both transport services and federated data services of third party federated data service providers over the broad communications network and at least one of the plurality of hotspots, as in claim 13.

The Office admits that Deshpande does not explicitly disclose a token operable as a valid indicator of access rights, as in claim 13. *See* Office Action, page 4. The Office asserts Barriga discloses this feature. *See* Office Action, page 4. Instead, the cited portions of Barriga utilize artifact authentication to authenticate a user to a single service provider (SP). *See* Barriga, paragraph [0066]. However, artifact authentication is different from the token-based authorization. Barriga's artifact does not indicate access rights to transport services and federated data services of federated service providers. Instead, Barriga's artifact method refers to a user's authentication assertion addressed for a single service provider. Thus, the artifact method does not disclose or suggest issuing a token indicating access rights to services of third party federated data service providers via the broad communications network, as in claim 13. Therefore, the cited portions of Deshpande and Barriga, separately or in combination, do not disclose or suggest at least one element of claim 13. Hence, claim 13 is allowable.

Claims 14-20 depend from claim 13, which Applicants have shown to be allowable. Therefore, claims 14-20 are also allowable, at least by virtue of their dependence from allowable claim 13.

CONCLUSION

Applicants have pointed out specific features of the claims not disclosed, suggested, or rendered obvious by the cited portions of the cited references as applied in the Office Action.

Accordingly, Applicants respectfully request reconsideration and withdrawal of each of the objections and rejections, as well as an indication of the allowability of each of the pending claims.

Any changes to the claims in this amendment, which have not been specifically noted to overcome a rejection based upon the cited art, should be considered to have been made for a purpose unrelated to patentability, and no estoppel should be deemed to attach thereto.

The Examiner is invited to contact the undersigned attorney at the telephone number listed below if such a call would in any way facilitate allowance of this application.

The Commissioner is hereby authorized to charge any fees, which may be required, or credit any overpayment, to Deposit Account Number 50-2469.

Respectfully submitted,

11-11-2008
Date

Jeffrey G. Toler, Reg. No. 38,342
Attorney for Applicant(s)
Toler Law Group, Intellectual Properties
8500 Bluffstone Cove, Suite A201
Austin, Texas 78759
(512) 327-5515 (phone)
(512) 327-5575 (fax)